REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggesstions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any oenalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
17-10-2008	Final Report	1-Sep-2005 - 31-Aug-2008

4. TITLE AND SUBTITLE
QCCM Center for Quantum Algorithms

5a. CONTRACT NUMBER
W911NF-05-1-0298

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

5d. PROJECT NUMBER
611102
OBXXX1

6. AUTHORS
Richard Cleve

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
MITACS
East Academic Annex, Rm. 120
Simon Fraser University
00000 -

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
49452-PH-QC.1

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
The goals of the project are to discover new quantum algorithms; develop novel paradigms for constructing quantum algorithms; develop complexity-theoretic results that relate to quantum algorithms; and develop theoretical approaches for the implementation of quantum algorithms.

Building on the pioneering work of Shor and Grover, the field of quantum algorithms has developed substantially, providing several insights about the underlying mechanisms behind quantum algorithms, as well as their limitations. Moreover, recent

15. SUBJECT TERMS
Quantum algorithms, quantum computing, fault-tolerant error correction

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Richard Cleve
U	U	U	SAR		19b. TELEPHONE NUMBER 519-888-4567

Standard Form 298 (Rev 8/98)
Prescribed by ANSI Std. Z39.18

Report Title

QCCM Center for Quantum Algorithms

ABSTRACT

The goals of the project are to discover new quantum algorithms; develop novel paradigms for constructing quantum algorithms; develop complexity-theoretic results that relate to quantum algorithms; and develop theoretical approaches for the implementation of quantum algorithms.

Building on the pioneering work of Shor and Grover, the field of quantum algorithms has developed substantially, providing several insights about the underlying mechanisms behind quantum algorithms, as well as their limitations. Moreover, recent work on novel paradigms for designing quantum algorithms (e.g., quantum walks and adiabatic computing), as well as theoretical advances relating algorithms to physical implementations (e.g., efficient error-correction techniques) point to promising directions for future development. Our focus is on searching for new algorithms and investigating the limitations of quantum information processing. Moreover, this is complemented by an investigation of quantum error-correction, the accuracy threshold for a variety of error models, focused on reducing overhead for implementations.

List of papers submitted or published that acknowledge ARO support during this reporting period. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

2006 Publications:

A nearly optimal discrete query quantum algorithm for evaluating NAND formulas
A. Ambainis 0704.3628v1

A New Quantum Lower Bound Method with Applications to Direct Product Theorms and Time-Space Tradeoffs
A. Ambainis, R. Spalek, R. de Wolf. quant-ph/0511200

Algebraic results on quantum automata
A. Ambainis, M. Beaudry, M. Golovkins, A. Kikusts, M. Mercer, D. Thrien
Theory of Computing Systems 39(2006), pages 165-188

Benchmarking Quantum Control Methods on a 12-Qubit System
C. Negrevergne, T.S. Mahesh, C.A. Ryan, M.J. Ditty, F. Cyr-Racine, W. Power, N. Boulant, T. Havel, D.G. Cory, R. Laflamme
Phys. Rev. Lett. 96, 170501 (2006)

Classical Interaction Cannot Replace a Quantum Message
D. Gavinsky quant-ph/0703215v2

Communicating over adversarial quantum channels using quantum list codes
Debbie Leung, Graeme Smith
IEEE Trans. Info. Theory 54, 2, 883-887 (2008) quant-ph/0605086

Discrete-query quantum algorithm for NAND trees
A. M. Childs and R. Cleve and S. P. Jordan and D. Yeung quant-ph/0702160v1

Exact and Approximate Unitary 2-Designs: Constructions and Applications
C. Dankert and R. Cleve and J. Emerson and E. Livine quant-ph/0606161v1

Exponential Separation of Quantum and Classical One-Way Communication Complexity for a Boolean Function
D. Gavinsky and J. Kempe and R. de Wolf quant-ph/0607174v1

Finding flows in the one-way measurement model
Niel de Beaudrap arXiv:quant-ph/0611284

Interaction in Quantum Communication
Hartmut Klauck, Ashwin Nayak, Amnon Ta-Shma, and David Zuckerman
quant-ph/0603135

Models of Quantum Cellular Automata
C. A. Perez-Delgado and D. Cheung
quant-ph/0508164v1

New Limits on Fault-Tolerant Quantum Computation
H. Buhrman and R. Cleve and M. Laurent and N. Linden and A. Schrijver and F. Unger
quant-ph/0604141v2

On the Role of Shared Entanglement
D. Gavinsky
quant-ph/0604052v2

Operator quantum error correction
D. W. Kribs and R. Laflamme and D. Poulin and M. Lesosky
Quant. Inf. & Comp., 6, 383 (2006)
quant-ph/0504189v3

Optimal quantum circuits for general phase estimation
W. van Dam and G. M. D'Ariano and A. Ekert and C. Macchiavello and M. Mosca
quant-ph/0609160v1

Phase map decompositions for unitaries
Niel de Beaudrap, Vincent Danos, Elham Kashefi
quant-ph/0603266

Polynomial degree vs. quantum query complexity
A. Ambainis
Journal of Computer and System Sciences, 72 (2006), pages 220-238

Quantum Algorithms and Complexity
M. Mosca
Proceedings of NATO ASI Quantum Computation and Information 2005, Chania, Crete, Greece, IOS Press (2006), in press

Quantum Cellular Automata and Single Spin Measurement
C. Perez, D. Cheung, M. Mosca, P. Cappellaro, D. Cory
Proceedings of Asian Conference on Quantum Information Science, Beijing, China

Quantum Circuit Simplification and Level Compaction
D. Maslov and G. W. Dueck and D. M. Miller
quant-ph/0604001v1

Quantum Complexity of Testing Group Commutativity
Frederic Magniez and Ashwin Nayak
quant-ph/0506265

Quantum Error Correcting Codes From The Compression Formalism
M. Choi and D. W. Kribs and K. Zyczkowski
Rep. Math. Phys., 58, 77 (2006) Quant-ph/0511101v2
Quantum Error Correcting Subsystems are Unitarily Recoverable Subsystems
D. W. Kribs and R. W. Spekkens
Phys. Rev. A 74, 042329 (2006)
quant-ph/0608045v2

Quantum search with variable times
A. Ambainis
quant-ph/0609168v1

Quantum Versus Classical Proofs and Advice
S. Aaronson and G. Kuperberg
quant-ph/0604056v3

Quantum Walk on a Line with Two Entangled Particles
Y. Omar, N. Paunkovic, L. Sheridan, S. Bose
Phys. Rev. A 74, 042304 (2006) quant-ph/0411065

Search via Quantum Walk
F. Magniez and A. Nayak and J. Roland and M. Santha
quant-ph/0608026v3

Self-Testing of Quantum Circuits
Frederic Magniez, Dominic Mayers, Michele Mosca, Harold Ollivier
Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP’06), Venice, Italy

Simple proof of fault tolerance in the graph-state model
P. Aliferis and D. W. Leung
Phys. Rev. A 73, 032308 (2006)
quant-ph/0503130v4

Strengths and Weaknesses of Quantum Fingerprinting
D. Gavinsky and J. Kempe and R. de Wolf
quant-ph/0603173v1

Strong Parallel Repetition Theorem for Quantum XOR Proof Systems
R. Cleve and W. Slofstra and F. Unger and S. Upadhyay
quant-ph/0608146v1

The Learnability of Quantum States
S. Aaronson
quant-ph/0608142v3

Toward a general theory of quantum games
G. Gutoski and J. Watrous
quant-ph/0611234v2

Two-way entanglement purification for finite block size
A. Ambainis, D. Gottesman.
IEEE Transactions on Information Theory, 52 (2006)

The minimum distance problem for two-way entanglement purification.
Andris Ambainis, Daniel Gottesman
IEEE Transactions on Information Theory, 52(2): 748-753 (2006)

Quantum algorithms for matching and network flows
A. Ambainis, R. Spalek.
Proceedings of STACS'06, Lecture Notes in Computer Science, 3884 (2006), pages 172-183. quant-ph/0508205

Quantum computing with highly mixed states.
Andris Ambainis, Leonard Schulman, Umesh Vazirani.
Journal of the ACM, 53:507-531 (2006).

Quantum direct product theorems for symmetric functions and time-space tradeoffs
A. Ambainis, R. Spalek, R. de Wolf.
quant-ph/0511200, combined version of this and the previous paper has been accepted to STOC'06.

QMA/qpoly is contained in PSPACE/poly: de-Merlinizing quantum protocols
S. Aaronson
Proceedings of IEEE Complexity 2006. quant-ph/0510230.

Oracles are subtle but not malicious
S. Aaronson
Proceedings of IEEE Complexity 2006. cs.CC/0504048.

Classical and quantum fingerprinting with shared randomness and one-sided error
R.T. Horn, A.J. Scott, J. Walgate, R. Cleve, A.I. Lvovsky, and B.C. Sanders
Quantum Information and Computation, 5(3), 258--271 (2005).

Quantum lower bounds for the Goldreich-Levin problem
M. Adcock, R. Cleve, K. Iwama, R. Putra, and S. Yamashita
Information Processing Letters, 97(5), 208--211 (2005).

Efficient quantum algorithms for simulating sparse Hamiltonians
D.W. Berry, G. Ahokas, R. Cleve, and B.C. Sanders
Accepted with minor revisions for publication in Communications in Mathematical Physics on 23 May 2006.

Additivity of quantum two-prover interactive proof systems
R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay.
Submitted 2006.

A unified and generalized approach to quantum error correction
D. Kribs, R. Laflamme, and D. Poulin.
Phys. Rev. Lett.

Pauli measurement are universal
V. Danos and E. Kashefi
Proceedings of the 3rd Workshop on Quantum Programming Languages, QPLO5 (2005).

Distributed measurement-based quantum computing
V. Danos, E. D'Hondt, E. Kashefi and P. Panangaden
Proceedings of the 3rd Workshop on Quantum Programming Languages, QPLO5 (2005).

Noiseless subsystems for collective rotation channels in quantum information theory
J.A. Holbrook, D. Kribs, R. Laflamme and D. Poulin
Integral Equations & Operator Theory, 51 (2) 215-234 (2005).

Lower Bounds on the Deterministic and Quantum Communication Complexities of Hamming-Distance Problems.
Andris Ambainis, William I. Gasarch, Aravind Srinivasan, Andrey Utis
Proceedings of ISAAC 2006, pp. 628-637

Improved Algorithms for Quantum Identification of Boolean Oracles.
Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Rudy Raymond Harry Putra, Shigeru Yamashita
Proceedings of SWAT 2006, pp. 280-291

Quantum Identification of Boolean Oracles. A chapter in H. Imai, M. Hayashi (eds.)
Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Rudy Raymond Harry Putra, Shigeru Yamashita
Quantum Computation and Information: From Theory to Experiment, Topics in Applied Physics, vol. 102, pp. 1-18 (2006)

Quantum walk algorithm for element distinctness.
Andris Ambainis
SIAM Journal on Computing, accepted for publication.

Approximate randomization of quantum states with fewer bits of key.
P. A. Dickinson and A. Nayak.
In Quantum Computing Back Action 2006, volume 864 of AIP Conference Proceedings, pages 18–36. Springer, New York, 2006. Refereed Volume.

Limits on the ability of quantum states to convey classical messages.
A. Nayak and J. Salzman.
Journal of the ACM, 53(1):184–206, Jan. 2006.

Invertible quantum operations and perfect encryption of quantum states.
A. Nayak and P. Sen.
Quantum Information and Computation, Jul. 2006. 7 pages.

Accessible versus holevo information for a binary random variable.
R. Jain and A. Nayak.

Technical Report quant-ph/0603278, ArXiv.org Preprint Archive, Mar. 2006. Submitted to Quantum Information and Computation. 7 pages.

Quantum key distribution based on arbitrarily-weak distillable entangled states
Karol Horodecki, Debbie W. Leung, Hoi-Kwong Lo, Jonathan Oppenheim
5 pages, double column (with page limit of 4) Journal Reference: Phys. Rev. Lett, 96 (2006) 070501.

Two-way quantum communication channels
Andrew M. Childs, Debbie W. Leung, Hoi-Kwong Lo
21 pages, single column
International Journal of Quantum Information, Memorial issue for Asher Peres 4 (2006) 63-83.

Fault-tolerant quantum computation in the graph-state model
Panos Aliferis, Debbie W. Leung
6 pages, double column (shortest derivation of that particular threshold theorem to-date)
Phys. Rev. A, 73 (2006) 032308.

Aspects of generic entanglement
Patrick M. Hayden, Debbie W. Leung, Andreas Winter
22 pages, single column
Comm. Math. Phys. 265 (2006) 95-117.

Typical entanglement of stabilizer states
G. Smith and D. Leung
10 pages, double column, quant-ph/0510232, in print for Phys. Rev. A.

Zero-knowledge against quantum attacks.
J. Watrous
Proceedings of the 38th ACM Symposium on Theory of Computing (STOC), pages 296–305, 2006.

Single spin measurement using cellular automata techniques
C. Perez, M. Mosca, P. Cappellaro, D. Cory
Physical Review Letters, (2006).

Witnessing effective entanglement in a continuous variable prepare & measure setup and application to a QKD scheme using postselection
S. Lorenz, J. Rigas, M. Heid, U.L. Andersen, N. Lütkenhaus, G. Leuchs
Phys. Rev. A 74, 042326 (2006) (9 pages)

Upper bound on the secret key rate distillable from effective quantum correlations with imperfect detectors
T. Moroder, M. Curty, N. Lütkenhaus
PRA 73, 012311 (2006) (9 pages)

Entanglement verification for quantum-key-distribution systems with an underlying bipartite qubit-mode structure
J. Rigas, O. Gühne, N. Lütkenhaus
PRA 73, 012341 (2006) (6 pages)

Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction
M. Heid and N. Lütkenhaus
PRA A 73, 052316 (2006) (7 pages)

Implementing Non-Projective Measurements via Linear Optics: an Approach Based on Optimal Quantum State Discrimination
P. van Loock, K. Nemoto, W. J. Munro, P. Raynal, N. Lütkenhaus
PRA 73, 062320 (2006) (13 pages)

2007 Publications:

Quantum network communication – the butterfly and beyond
D. Leung, J. Oppenheim and A. Winter
13 pages, double column, quant-ph/0608223 accepted for presentation in QIP 2007

An extremal result for geometries in the one-way measurement model
Niel de Beaudrap, Martin Pei
To appear in QIC
arXiv:quant-ph/0702229

Direct Product Theorems for Communication Complexity via Subdistribution Bounds
Rahul Jain, Hartmut Klauck, and Ashwin Nayak
ECCC Technical Report TR07-064

Distinguishing Short Quantum Computations
Bill Rosgen
STACS 2008
arXiv:0712.2595v1

Efficient quantum algorithms for simulating sparse Hamiltonians
D. W. Berry and G. Ahokas and R. Cleve and B. C. Sanders
Comm. Math. Phy. 270, 359 (2007)
quant-ph/0508139v2

Entanglement-Resistant Two-Prover Interactive Proof Systems and Non-Adaptive Private Information Retrieval Systems
R. Cleve and D. Gavinsky and R. Jain
0707.1729v1

Experimentally scalable protocol for identification of correctable codes
Marcus Silva, Easwar Magesan, David W. Kribs, Joseph Emerson
arXiv:0710.1900

Exponential Separation of Quantum and Classical Non-Interactive Multi-Party Communication Complexity
D. Gavinsky and P. Pudl\'ak
0708.0859v1

General optimized schemes for phase estimation
G. M. D’Ariano, W. van Dam, E. Ekert, C. Macchiavello, and M. Mosca
Physical Review Letters, Volume 98, Number 9, Article 090501

Generalization of Quantum Error Correction via the Heisenberg Picture and Application to Information Flow
Cedric Beny, Achim Kempf, David W. Kribs
Phys. Rev. Lett. 98, 100502 (2007)
quant-ph/0608071

Interaction in Quantum Communication
Hartmut Klauck, Ashwin Nayak, Amnon Ta-Shma, and David Zuckerman
IEEE Transactions on Information Theory, 53(6), pages 1970--1982, June 2007

Limitations of some simple adiabatic quantum algorithms
L. M. Ioannou and M. Mosca
quant-ph/0702241v1

Linear Depth Stabilizer and Quantum Fourier Transformation Circuits with no Auxiliary Qubits in Finite Neighbor Quantum Architectures
D. Maslov
quant-ph/0703211v1

Local Unitary Quantum Cellular Automata
Carlos A. Pérez-Delgado and Donny Cheung
Phys. Rev. A 76, 032320 (2007) (15 pages)
arXiv:0709.0006

Optimal phase estimation in quantum networks
G. M. D'Ariano, W. van Dam, E. Ekert, C. Macchiavello, and M. Mosca
Journal of Physics A: Math. Theor. 40, 7971-7984

Quantum Circuit Placement: Optimizing Qubit-to-qubit Interactions through Mapping Quantum Circuits into a Physical Experiment
D. Maslov, S. M. Falconer, and M. Mosca
Proceedings of ACM/IEEE Design Automation Conference, pp. 962-966, San Diego, CA, 2007
quant-ph/0703256

Quantum Complexity of Testing Group Commutativity
Frederic Magniez and Ashwin Nayak
Algorithmica, 48(3), pages 221--232, 2007

Quantum t-designs: t-wise independence in the quantum world
A. Ambainis and J. Emerson
quant-ph/0701126v2

Search via Quantum Walk
Frederic Magniez, Ashwin Nayak, Jeremie Roland, and Miklos Santha
In Proceedings of the Thirty-Ninth Annual ACM Symposium on the Theory of Computing, 575 - 584, 2007

Self-testing of universal and fault-tolerant sets of quantum gates
W. van Dam, F. Magniez, M. Mosca and M. Santha
SIAM Journal on Computing, Vol. 37, No. 2
611-629 (2007)

Perfect Parallel Repetition Theorem for Quantum XOR Proof Systems
R. Cleve, W. Slofstra, F. Unger and S. Upadhyay
In Proceedings of the 22nd IEEE Conference on Computational Complexity (CCC), pages 109–114, 2007.

Toward a general theory of quantum games
G. Gutoski and J. Watrous
In Proceedings of the 39th ACM Symposium on Theory of Computing (STOC'07), pages 565–574, 2007.

An Introduction to Quantum Computation
P. Kaye, R. Laflamme, M. Mosca
Oxford University Press, (ISBN: 0198570007).

Checking Matrix Identities
A. Nayak
Encyclopedia of Algorithms. 4 pages.

A Separation between Divergence and Holevo Information for Ensembles
Rahul Jain, Ashwin Nayak, and Yi Su.
Technical Report arXiv:0712.3867. Submitted to TAMC 08, December, 2007. 13 pages.

Symmetrized Characterization of Noisy Quantum Processes
J. Emerson, M. Silva, O. Moussa, C. Ryan, M. Laforest, J. Baugh, D. Cory, R. Laflamme
Science 317, pp. 1893-1896 (2007).

Signatures of Incoherence in a Quantum Information Processor

M. K. Henry, A. Gorshkov, Y.Weinstein, P. Cappellaro, J. Emerson, Nicolas Boulant, Jonathan S. Hodges, Chandrasekhar Ramanathan, Timothy F. Havel, Rudy Martinez and David G. Cory
Quantum Information Processing 6, 431-444 (2007).

Efficient Error Characterization in Quantum Information Processing
B. Lévi, C. C. López, J. Emerson, and D. G. Cory
Phys. Rev. A 75, 022314 (10 pages) (2007).

Symmetrisation Methods for Characterisation and Benchmarking of Quantum Processes
J. Emerson
Conference Proceedings for Theory Canada 4, Canadian Journal of Physics.

Scalable Experimental Protocol for Identification of Correctable Codes
M. Silva, E. Magesan, D. Kribs, and J. Emerson
Submitted to Phys. Rev. Lett. (2007).

Unconditional Security for Practial
H. Inamori, N.Lütkenhaus, and D. Mayers
Quantum Key Distribution; European Physical Journal D. Vol 41, p. 599 (2007)

On experimental procedures for entanglement verification
S.J. van Enk, N. Lütkenhaus, H.J. Kimble
Phys. Rev. A, Vol. 75, 052318 (2007)

Zero-Error Attacks and Detection Statistics in the Coherent One-Way Protocol for Quantum Cryptography
C. Branciard, N. Gisin, N. Lütkenhaus, V. Scarani
Quantum Information and Computation, Vol. 7, p. 639-664, 2007.

Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states
M. Curty, L.-L. Zhan, H.-K. Lo, N. Lütkenhaus
Quantum Information and Computation, Vol 7, p 665-688, 2007.

Security of coherent state quantum cryptography in the presence of Gaussian noise
M. Heid, N. Lütkenhaus
Phys. Rev. A 76, 022313 (2007)

Optimal unambiguous state discrimination of two density matrices: A second class of exact solutions
Ph. Raynal, N. Lütkenhaus
Phys. Rev. A, Vol 76, 052322, 2007.

2008 Publications:

Optimizing the discrete time quantum walk using a SU(2) coin
C. M. Chandrashekar, R. Srikanth, and Raymond Laflamme
Phys. Rev. A 77, 032326 (2008)
arXiv:0711.1882

Additivity and Distinguishability of Random Unitary Channels
Bill Rosgen
arXiv:0804.1936v1

Direct product theorems for classical communication complexity via subdistribution bounds
Rahul Jain, Hartmut Klauck, Ashwin Nayak
The 40th ACM Symposium on Theory of Computing (STOC) 2008

New bounds on classical and quantum one-way communication complexity
Rahul Jain, Shengyu Zhang
arXiv:0802.4101v1

Quantum Circuit Placement
D. Maslov, S. M. Falconer, and M. Mosca
IEEE Transactions on CAD 27(4):752-763, April 2008
quant-ph/0703256

Quantum Circuit Simplification and Level Compaction
D. Maslov, G. W. Dueck, D. M. Miller, and C. Negrevergne
IEEE Transactions on CAD, 27(3):436-444, March 2008

Towards a world with quantum computers
D. Bacon, D. Leung
Comm. ACM, 50(9), 55 (2008)

The power of quantum systems on a line
D. Aharonov, D. Gottesman, S. Irani, and J. Kempe
Proc. 48th IEEE Symposium on the Foundations of Computer Science (FOCS), pp. 373-383 (2007).

Universal computation by quantum walk
A. M. Childs
arXiv:0806.1972.

Optimal quantum adversary lower bounds for ordered search
A. M. Childs and T. Lee
Proc. 35th International Colloquium on Automata, Languages and Programming, Lecture Notes in Computer Science 5125, pp. 869-880 (2008).

An exponential separation between the entanglement and communication capacities of a bipartite unitary interaction
A. Harrow and D. Leung
arXiv:0803.3066.

Coherent state exchange in multi-prover quantum interactive proof systems
D. Leung, B. Toner, and J. Watrous
arXiv: 0804.4118.

Quantum computational complexity
J. Watrous
arXiv: 0804.3401. To appear in Encyclopedia of Complexity and System Science, Springer, 2008.

Distinguishing quantum operations with few Kraus operators
J. Watrous
arXiv: 0710.0902. To appear in Quantum Information a

Number of Papers published in peer-reviewed journals: 78.00

(b) Papers published in non-peer-reviewed journals or in conference proceedings (N/A for none)

Number of Papers published in non peer-reviewed journals: 0.00

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts): 0

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts): 0

(d) Manuscripts

Number of Manuscripts: 0.00

Number of Inventions:

Graduate Students

NAME	PERCENT_SUPPORTED
Sevag Gharibian	0.08
William Rosgen	0.08
Ansis Rosmanis	0.08
Lana Sheridan	0.08
Sarvagya Upadhyay	0.08
Nathan Wiebe	0.06
David Yonge-Mallo	0.08
FTE Equivalent:	**0.54**
Total Number:	**7**

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
Rahul Jain	0.60
Dmitri Maslov	0.08
André Methot	0.08
Rolando Somma	0.00
Dmitry Gavinsky	0.65
Scott Aaronson	0.60
FTE Equivalent:	**2.01**
Total Number:	**6**

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Richard Cleve	0.00	No
Michele Mosca		No
Daniel Gottesman		No
Debbie Leung		No
Andrew Childs		No
Raymond Laflamme		No
John Watrous		No
Ashwin Nayak		No
Andris Ambainis		No
Peter Hoyer		No
Barry Sanders		No
David Kribs	0.25	No
Joseph Emerson		No
FTE Equivalent:	**0.25**	
Total Number:	**13**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:...... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:...... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):...... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:...... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:...... 0.00

Names of Personnel receiving masters degrees

NAME	
Heath Gerhard	
William Rosgen	
Christoph Dankert	
Nathan Wiebe	
Total Number:	**4**

Names of personnel receiving PHDs

NAME	
Dmitry Gavinsky	
Donny Cheung	
Phillip Kaye	
Carlos Perez-Delgado	
Casey Myers	
David Poulin	
Total Number:	**6**

Names of other research staff

NAME	PERCENT_SUPPORTED	
Wendy Reibel	0.00	No
Meghan Huras		No
Lorna Kropf		No
FTE Equivalent:	**0.00**	
Total Number:	**3**	

Sub Contractors (DD882)

Inventions (DD882)

1. Statement of the Problems Studied

The goal of the project is to discover new quantum algorithms; develop novel paradigms for constructing quantum algorithms; develop complexity-theoretic results that relate to quantum algorithms; and develop theoretical approaches for the implementation of quantum algorithms.

2. Summary of the Most Important Results

- We have contributed to the development of fast quantum algorithms for evaluating AND-OR trees (a.k.a. NAND trees), which are relevant in the context of evaluating optimal strategies in interactive settings (including various games). In particular, we showed how to obtain efficiency $O(N^{1/2+\varepsilon})$ for any $\varepsilon > 0$ in the discrete query setting, as well as how to generalize from balanced AND-OR trees to arbitrary AND-OR trees in the discrete query setting.
- We have extended the AND-OR results to algorithms for evaluating MIN-MAX trees.
- We have discovered an efficient quantum algorithm for searching among N items when the costs of querying the individual items are different. The algorithm runs in time $O(\sqrt{T})$, where T is the sum of the squares of the query times.
- In the area of lower bounds for algorithms, we have developed a new and more powerful variant of the adversary lower bound method, to handle negative weights.
- Finally, we have discovered a new efficient procedure for generating t-designs (which, roughly speaking, can be thought of as t^{th} order pseudorandom quantum states).
- We have shown that every quantum algorithm can be simulated by a continuous-time quantum walk of a simple form, and the methodology (using “widgets”) may lead to other applications in quantum algorithm design.
- We have clarified some notions about the “hitting times” for quantum walks (the time that it takes to get from one vertex to another), showing a quadratic speedup in the quantum case for a broad class of graphs.
- We have derived some improved quantum algorithms for simulating Hamiltonians that were previously known only for the sparse case.
- In the continuous-time query algorithmic paradigm (which is the paradigm where last year’s breakthrough result about NAND trees was first discovered), we have a general method for simulating a time T algorithm by a discrete quantum algorithm in time $O(T \log T)$. Previously, efficient simulations were known for some specific continuous-time algorithms; it was an open question whether this is always possible (a paper is forthcoming).
- Progress was made on an ongoing project concerning a quantum algorithm for the ferromagnetic Ising model (a paper is forthcoming).
- Regarding algorithms pertaining to quantum computing problems, we have further investigated the hardness of determining whether a bipartite quantum state (specified as a density matrix) is separable or entangled. This problem has long been known to be NP-hard—and thus likely hard even for quantum computers. However, the previous NP-hardness actually showed the problem is NP-hard in the case where exponential precision is required. This means that even entangled

states that are exponentially close to the separable region must be identified as entangled (even though their entanglement is exponentially small). We have shown that the problem remains NP-hard even if the precision is relaxed so as to be polynomial (as opposed to exponential). What this means is that it is unlikely that there is an efficient algorithm even for the problem of distinguishing separable states from those whose entanglement is significant (inverse polynomial in size).

- Finally, we have discovered a distributed computing problem that requires infinite entanglement to accomplish perfectly (and arbitrarily large entanglement to accomplish with arbitrary precision). This helps to explain why several complexity theoretic questions about multi-prover interactive proof systems have been very difficult to resolve: the underlying space of possible entangled states is not compact, and hence difficult to characterize in simple mathematical terms.

3. Bibliography

D. Aharonov, **D. Gottesman**, S. Irani, and J. Kempe, "The power of quantum systems on a line," Proc. 48th IEEE Symposium on the Foundations of Computer Science (FOCS), pp. 373-383 (2007).

A. Ambainis, "Quantum search with variable times", manuscript at quant-ph/0609168.

A. Ambainis, **A. M. Childs**, B. W. Reichardt, R. Špalek, and S. Zhang, "Any AND-OR formula of size N can be evaluated in time $N^{1/2+o(1)}$ on a quantum computer", Proc. 48th IEEE Symposium on Foundations of Computer Science, pp. 363-372 (2007).

A. Ambainis and **J. Emerson**. "Quantum t-designs: t-wise independence in the quantum world". Proceedings of *Complexity '07*, pages 129–140.

G. M. D'Ariano, W. van Dam, E. Ekert, C. Macchiavello, and **M. Mosca**, "Optimal phase estimation in quantum networks", *Journal of Physics A: Math. Theor.* 40 (2007).

G. M. D'Ariano, W. van Dam, E. Ekert, C. Macchiavello, and **M. Mosca**, "General optimized schemes for phase estimation". *Physical Review Letters*, Vol. 98, No. 9, Article 090501 (2007).

D. Berry, G. Ahokas, **R. Cleve**, and **B. Sanders**, "Efficient quantum algorithms for simulating sparse Hamiltonians", *Communications in Mathematical Physics* 270(2): 359–371 (2007).

C. M. Chandrashekar, R. Srikanth, and **R. Laflamme**. "Optimizing the discrete time quantum walk using a SU(2) coin", Phys. Rev. A 77, 032326 (2008).

A. M. Childs. "Universal computation by quantum walk", arXiv:0806.1972.

A. M. Childs, **R. Cleve**, S. P. Jordan, and **D. L. Yeung**, "Discrete-query quantum algorithm for NAND trees", arXiv:quant-ph/0702160.

A. M. Childs and T. Lee. "Optimal quantum adversary lower bounds for ordered search", Proc. 35th International Colloquium on Automata, Languages and Programming, Lecture Notes in Computer Science 5125, pp. 869-880 (2008).

R. Cleve, **D. Gavinsky**, and **R. Jain**, "Entanglement-Resistant Two-Prover Interactive Proof Systems and Non-Adaptive Private Information Retrieval Systems", arXiv:0707.1729.

R. Cleve, **D. Gavinsky**, and **D. L. Yeung**, "Quantum Algorithms for Evaluating MIN-MAX Trees", arXiv:0710.5794.

R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay, "Perfect Parallel Repetition Theorem for Quantum XOR Proof Systems", In *Proceedings of the 22nd IEEE Conference on Computational Complexity (CCC)*, pages 109–114, 2007.

S. Gharibian, "On the Hardness of the Quantum Separability Problem and the Global Power of Locally Invariant Unitary Operations", Master's thesis, University of Waterloo, 2008.

W. van Dam, F. Magniez, **M. Mosca**, and M. Santha, "Self-testing of universal and fault-tolerant sets of quantum gates", *SIAM Journal on Computing*, Vol. 37, No. 2, 611–629 (2007).

G. Gutoski and **J. Watrous**. "Toward a general theory of quantum games". In *Proceedings of the 39th ACM Symposium on Theory of Computing (STOC'07)*, pages 565–574, 2007.

A. Harrow and **D. Leung**. "An exponential separation between the entanglement and communication capacities of a bipartite unitary interaction", arXiv:0803.3066.

P. Høyer, T. Lee, and R. Spalek. "Negative weights make adversaries stronger", *Proceedings of the 39th ACM Symposium on Theory of Computing (STOC'07)*, pages 526–535, 2007.

R. Jain, H. Klauck, and **A. Nayak**. "Direct Product Theorems for Communication Complexity via Subdistribution Bounds." Manuscript submitted to ECCC, June 2007.

R. Jain, **A. Nayak**, and Yi Su. "A separation between divergence and Holevo information for ensembles", arXiv: 0712.3867.

P. Kaye, **R. Laflamme**, and **M. Mosca**, *An Introduction to Quantum Computation*, Oxford University Press, (ISBN: 0198570007).

D. Leung, B. Toner, and **J. Watrous**. “Coherent state exchange in multi-prover quantum interactive proof systems”, arXiv: 0804.4118.

F. Magniez and **A. Nayak**. “Quantum Complexity of Testing Group Commutativity.” *Algorithmica*, 48(3), pages 221–232, 2007.

D. Maslov, S. M. Falconer, and **M. Mosca**. “Quantum Circuit Placement: Optimizing Qubit-to-qubit Interactions through Mapping Quantum Circuits into a Physical Experiment”. *Proceedings of ACM/IEEE Design Automation Conference (DAC)*, San Diego, CA, (2007).

A. Nayak. “Checking Matrix Identities”, *Encyclopedia of Algorithms*. To appear.

A. Nayak and P. Sen. “Invertible Quantum Operations and Perfect Encryption of Quantum States.” *Quantum Information and Computation*, 7(1), pages 103–110, January 2007.

J. Watrous. “Quantum computational complexity”, arXiv: 0804.3401. To appear in Encyclopedia of Complexity and System Science, Springer, 2008.

J. Watrous. “Distinguishing quantum operations with few Kraus operators”, arXiv: 0710.0902. To appear in Quantum Information and Computation.